BIS

Anche il Generale Custer raccoglie le frecce.

Acquista i grandi successi della Linea BIS.
Accumula i "Punti Freccia" e scegli i tuoi premi dal nostro catalogo.

Maggiori dettagli sul sito

www.lineabis.it

www.dde.it

Contenuto del CD

Ecco l'elenco di tutti i programmi nel CD divisi per sezione e con l'indicazione della cartella dove trovarli.

LEGENDA

- C PROGRAMMA COMPLETO
- F PROGRAMMA GRATUITO
- D PROGRAMMA DEMO

2 PROGRAMMI COMPLETI!

Ulead DVD MovieFactory 2
Programma completo per masterizzare filmati, immagini e musica su CD e DVD. Durante l'installazione del software inseriamo il codice **221A2-62000-00355906** quando richiesto.

OpenOffice.Org 2.0.1
La nuova versione della raccolta di programmi completi e in italiano per l'ufficio e per la casa. Comprende un software per scrivere testi, gestire tabelle, creare presentazioni e disegnare.

CREATIVITÀ

D Advanced GIF Animator 2.23
Advanced GIF Animator consente di creare GIF animate.

D Paint Shop Pro X
Il famoso software per ritoccare le immagini.

F PhotoFiltre 6.2.3
Un software per applicare effetti grafici alle immagini.

D Ulead DVD MovieFactory 4.0
Per personalizzare i filmati e trasferirli su DVD.

F Cruci LAB 2005 v.5.0
Per creare cruciverba e divertirsi con gli amici.

F MediaPortal 0.2 RC2
La versione gratuita per trasformare il PC in un Media Center con cui guardare filmati e ascoltare musica.

INTERNET

F aMSN 0.95
Un clone di MSN Messenger con tante funzioni per inviare messaggi ai nostri amici.

F Download Express 1.9
Si integra in Internet Explorer e Firefox per effettuare download multipli di file.

F Internet Connection B. 3.5.0
Permette di velocizzare l'invio e la ricezione delle email.

F LeechGet 2005 v.1.5
Per scaricare file e migliorare la navigazione in Rete.

F MozBackup 1.4.3
Effettua il backup di Firefox, Thunderbird e Mozilla Suite.

F VisualIRC 2.0
Un ottimo programma gratuito per chattare e conoscere nuove persone.

UTILITY

F Arovax Shield 1.2.314
Programma gratuito per proteggere il computer dai programmi spyware.

F Bazooka 1.13.03
Verifica la presenza di oltre 460 spyware e li elimina.

D BullGuard 6.0
Protegge il computer tramite il firewall, elimina i virus ed effettua il backup dei dati.

F CD BurnerXP Pro 3.0.116
Software gratuito per masterizzare CD e DVD.

F CWShredder 2.19
Elimina il virus CoolWebSearch che modifica la pagina iniziale di Internet Explorer.

F CryptoMX Tools 1.58
Per crittografare e stenografare i nostri dati personali.

F IE Privacy Keeper 2.7.3
Consente di eliminare i cookie e i file temporanei di Internet Explorer.

F LockNote 1.0.2
Per proteggere con password i nostri appunti di testo.

D Norton Internet Security 2006
Controlla la navigazione in Rete dei minori.

F QuickZip 4.60.014
Permette di comprimere e decomprimere i file.

F TrueCrypt 4.1
Per crittografare e proteggere i file presenti nel computer.

F XP-Antispy 3.95-2
Configura e modifica le impostazioni di Windows XP.

...E MOLTO ALTRO ANCORA

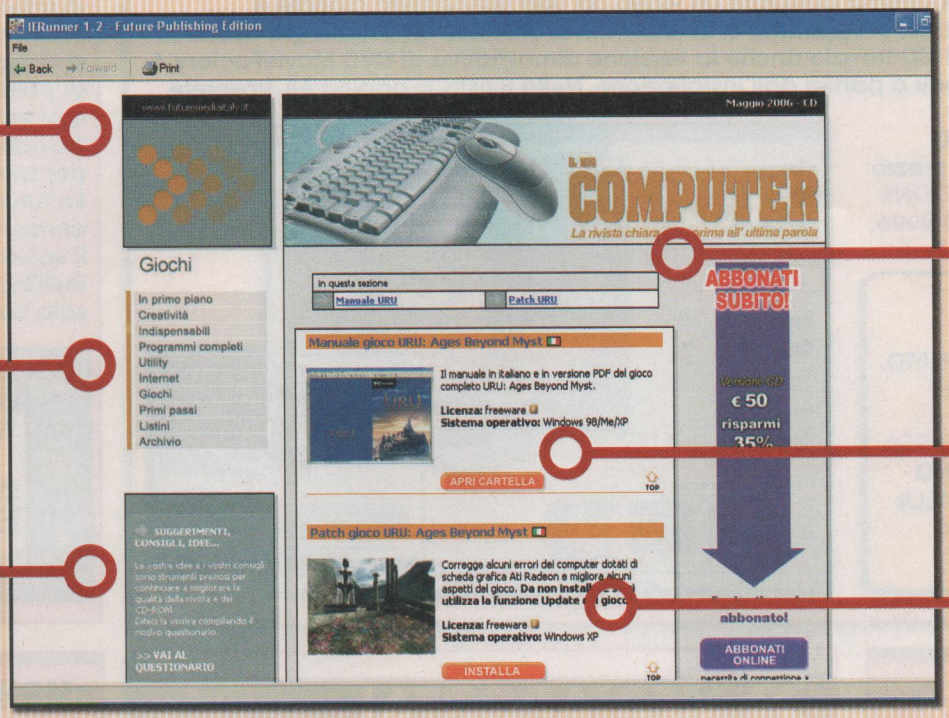
COME USARE IL CD

Se il nostro computer legge automaticamente i CD-ROM, basterà inserire il CD nel lettore e aspettare l'avvio automatico del disco. Se invece il CD-ROM non si avvia, apriamo la cartella Risorse del Computer, con il tasto destro del mouse clicchiamo sull'icona Mico05CD e dal menu che compare scegliamo la voce Esplora. Per avviare il CD facciamo doppio clic sull'icona IERunner.exe. Qui di seguito, invece, scopriamo come navigare tra i menu del CD.

HOME
Se clicchiamo su questo pulsante, torniamo alla pagina principale del CD.

SEZIONI
Per navigare nel CD, dobbiamo cliccare sui nomi delle varie sezioni.

QUESTIONARIO
Per compilare il questionario online de Il Mio Computer.



PROGRAMMI
Qui sono elencati tutti i programmi inclusi nella sezione.

INSTALLARE
Per installare il programma o aprire la cartella che contiene il software.

INFORMAZIONI
Tutte le specifiche del programma e un sunto delle sue caratteristiche.

INDISPENSABILI

Ad-aware SE PE 1.06
Per individuare e rimuovere i programmi chiamati spyware che violano la nostra privacy.

Adobe Reader 7.0.7
Per visualizzare e stampare i file in formato PDF. Attenzione: funziona solo con Windows XP.

Firefox 1.5.0.1
Il software per navigare in Rete, gratuito e in italiano, alternativo a Internet Explorer.

GTK+ 2 for Windows 2.8.9
Una serie di librerie per utilizzare alcuni programmi gratuiti.

IrfanView 3.98
Programma gratuito per visualizzare le immagini.

IrfanView 3.98 Italiano
Per usare il programma in italiano copiamo nella cartella chiamata **Languages** il file italian.dll. Avviamo il programma e selezioniamo italiano dalla voce **Change Language** del menu *Options*.

Java 2 Runtime 5.0 update 6
Indispensabile per navigare in Rete e visualizzare le animazioni sviluppate con la tecnologia Java.

Mozilla Thunderbird 1.5
Un ottimo programma per gestire la posta elettronica: gratis e tutto in italiano.

Orphan Remover 1.8.9
Elimina i collegamenti non più riferiti a file o cartelle.

Spybot Search & Destroy 1.4
Utilizziamo questo programma gratuito in italiano per individuare e rimuovere i pericolosi programmi spyware.

Winamp 5.21
La nuova versione del programma per ascoltare la musica e guardare i video musicali.

XviD 1.1.0
L'ultima versione dei driver più utilizzati per la compressione dei filmati video in formato XviD.

ZipGenius 6.0.2 Standard Ed.
Questo software permette di gestire qualsiasi tipo di file compresso. Utile per i file più ingombranti.

SE IL CD NON FUNZIONA

Ogni mese, con le riviste di Future Media Italy, arrivano nelle edicole centinaia di migliaia di CD. Può capitare che alcuni di questi si rovinino rompendosi o diventando illeggibili. In tal caso, è possibile richiedere la sostituzione gratuita del CD inviando quello danneggiato a Future Media Italy, via Asiago 45 - 20128 Milano entro 90 giorni dalla data di pubblicazione. È importante indicare le proprie generalità e il recapito al quale si vuole ricevere il CD. Per altre informazioni scrivete a: reception@futureitaly.it oppure inviate un fax al numero 02.260.055.20.

ULEAD DVD MOVIEFACTORY

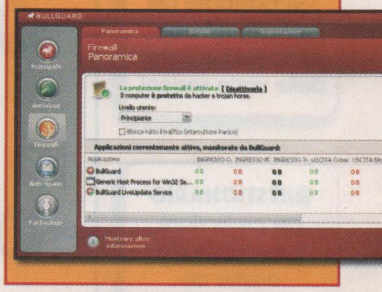
PROGRAMMA COMPLETO

Ulead DVD MovieFactory 2 è un programma completo per creare i nostri DVD con contenuti video, audio e testi. Il software è composto da quattro moduli. La funzione principale è *Start Project*, che permette di creare un nuovo progetto scegliendo tra DVD, VCD e SVCD o di modificarne uno creato in precedenza. Se scegliamo di realizzare un DVD, potremo catturare un video da una telecamera digitale e importarlo all'interno del programma o, in alternativa, utilizzare un filmato già esistente e personalizzarlo. Nel CD trovate anche la versione dimostrativa di DVD MovieFactory 4, utilizzabile per 30 giorni a partire dall'installazione. Nella rivista, a pagina 68, troverete un buono sconto per acquistare Ulead DVD MovieFactory 4 a un prezzo scontato. **LA PROMOZIONE SCADE IL 30 GIUGNO 2006.**

ATTENZIONE:
PER REGISTRARE IL PROGRAMMA COMPLETO, DOBBIAMO INSERIRE QUESTO CODICE: 221A2-62000-00355906 E RIMUOVERE IL SEGNO DI SPUNTA DAVANTI ALLA VOCE Register Ulead DVD MovieFactory 2.

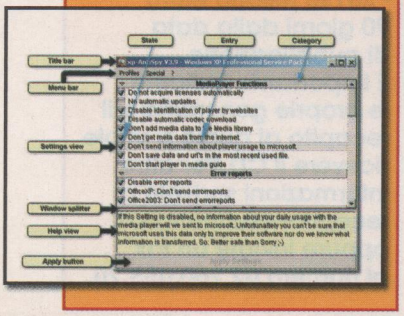
BULLGUARD

Un software in versione dimostrativa e in italiano per proteggere il nostro computer. Troveremo il firewall per navigare in Internet in totale sicurezza, e l'antivirus che si integra nel programma di posta elettronica e ci protegge dai virus. Troviamo anche il filtro per bloccare lo spam. La funzione **Fai backup** consente di organizzare il salvataggio dei dati. BullGuard 6 funziona solo con Windows XP.



XP-ANTISPY

Un utile programma, gratuito e in italiano, per cambiare le impostazioni di Windows XP. Dal menu *Profili*, selezionando la voce **Impostazioni predefinite di sistema**, potremo ripristinare Windows alle condizioni iniziali o scegliere un'altra opzione tra quelle disponibili. Per configurare Windows XP, scegliamo una delle funzioni in grigio e premiamo **Applicare le impostazioni** per rendere effettive le modifiche.

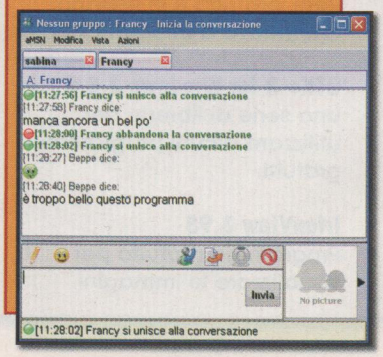


MEDIAPORTAL

MediaPortal è la versione simile a XP Media Center Edition, dal quale riprende l'aspetto e alcune funzioni. Installando questo software potremo trasformare il nostro computer in una postazione multimediale e guardare filmati, ascoltare canzoni e molto altro ancora. La versione presente nel CD funziona solo con il sistema operativo Windows XP. **Prima di usare MediaPortal, è necessario installare il software Microsoft .NET Framework 2.0, scaricabile dalla sezione *download* del sito Internet www.microsoft.com/italy.**

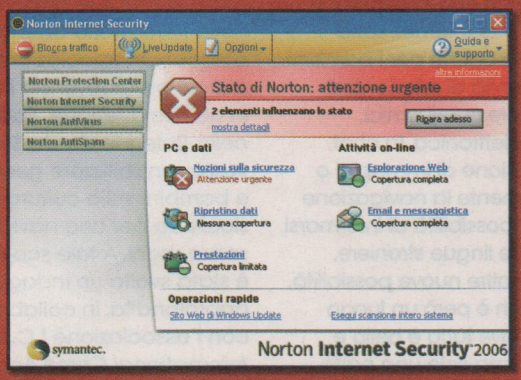
aMSN

Il clone del più famoso MSN Messenger, per inviare messaggi istantanei e immagini ai nostri amici collegati a Internet. Accediamo a aMSN inserendo l'indirizzo di posta elettronica di Hotmail e la relativa password. Nel menu *Strumenti* scegliamo la voce **Preferenze** per personalizzare le impostazioni di aMSN. Selezioniamo **Italian** durante l'installazione di aMSN per usare il programma in italiano.



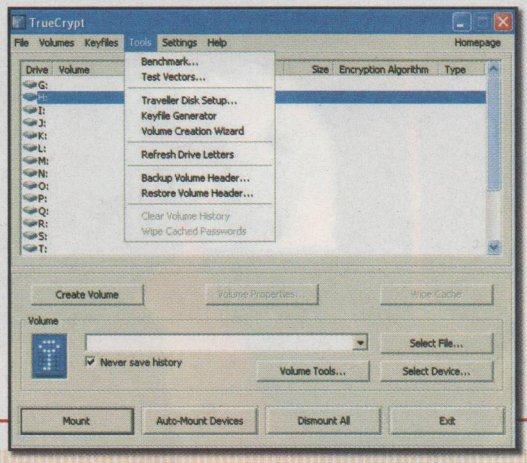
SICUREZZA IN RETE

Proteggiamo il nostro computer e navighiamo con tranquillità con la versione dimostrativa di Norton Internet Security 2006, in italiano e per Windows XP. Troviamo Norton AntiSpam per bloccare e cancellare la posta elettronica indesiderata e Norton Parental Control per proteggere i bambini durante la navigazione in Internet. Avremo inoltre a disposizione un potente firewall e Norton AntiVirus per riconoscere ed eliminare tutti i virus. Per conoscere meglio le funzioni di Norton Internet Security 2006 seguiamo la guida a pagina 92 della rivista.

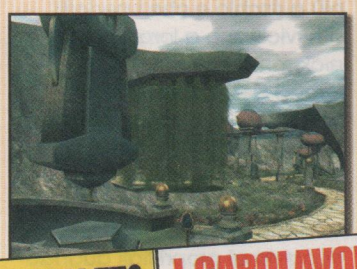


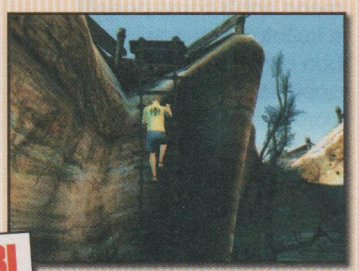
CRITTOGRAFIA

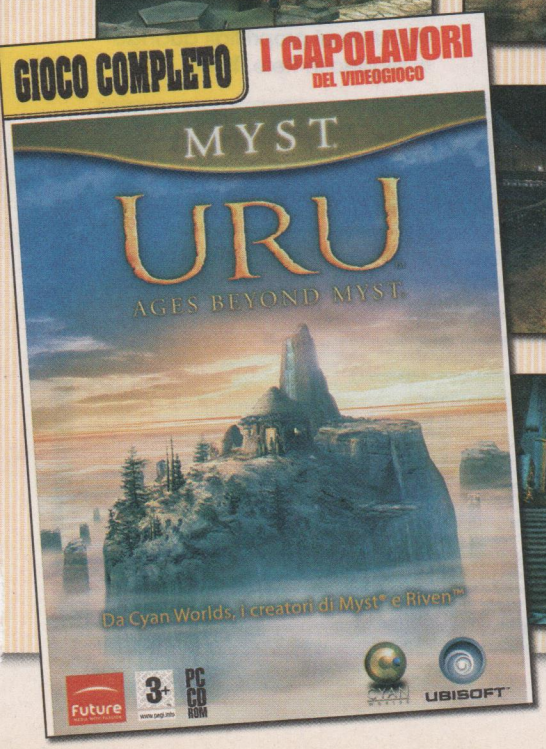
Nel CD di questo mese troviamo una raccolta di programmi gratuiti per crittografare i file presenti nel disco fisso del nostro computer. In questo modo i nostri dati saranno protetti e al sicuro da occhi indiscreti. CryptoMX Tools utilizza la tecnologia Java per stenografare i file, mentre con TrueCrypt potremo crittografare i dati utilizzando potenti metodi di protezione. **TrueCrypt funziona solo con il sistema operativo Windows XP.** Windows Privacy Tools unisce alcuni programmi per la crittografia e la firma digitale.

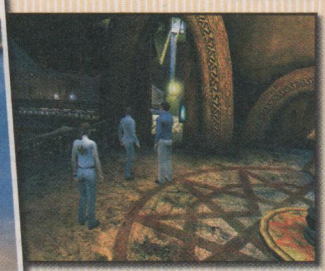


GIOCO COMPLETO



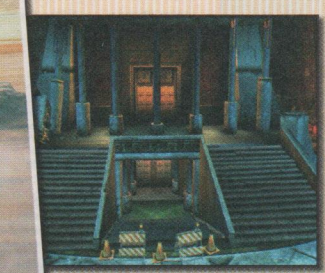


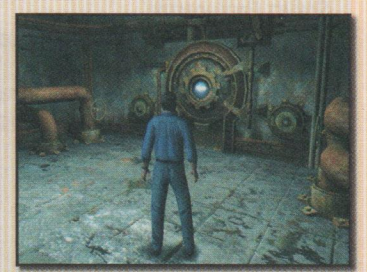




URU: AGES BEYOND MYST UN FANTASTICO GIOCO COMPLETO IN ITALIANO!

Spiegare in poche parole la saga di Myst è un'impresa impossibile. Cinque capitoli e numerose edizioni nel corso di tredici anni, oltre dieci milioni di giocatori e un primato di copie vendute che ha resistito per lunghissimo tempo, nonostante il progresso e le nuove tecnologie. Nel gioco URU: Ages Beyond Myst saremo nei panni di una persona reale che viene convocata da un gruppo di archeologi per partecipare all'esplorazione delle rovine di una civiltà dimenticata. Questa civiltà, altro non è che quella D'ni, la cui storia è la base dei cinque giochi della serie originale. Nel CD dei programmi troviamo il manuale in italiano e una patch per correggere alcuni errori del gioco.





Il Web per i piccoli

Internet contiene opportunità e, purtroppo, nuovi pericoli. Ecco come difendersi da pedofilia e abusi senza inutili rinunce.

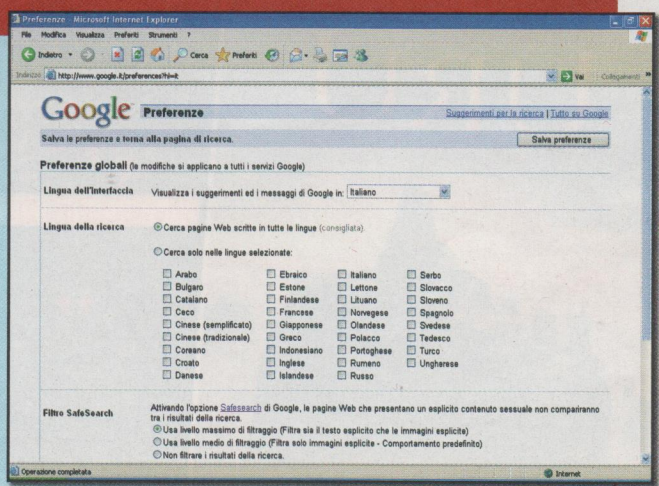
Con l'avvento delle nuove tecnologie e con la diffusione di Internet, sono aumentate anche per i bambini le opportunità di relazionarsi e conoscere nuovi amici. La posta elettronica, la chat, la condivisione di immagini o semplicemente la navigazione offrono la possibilità di informarsi, imparare le lingue straniere, giocare e altre nuove possibilità. La Rete non è però un luogo magico dove tutto è bello e incantato, ma solo una parte della realtà che incontriamo nella vita di tutti i giorni. Possiamo trovare tantissime persone oneste e disinteressate, ma anche personaggi molto meno nobili come pedofili e truffatori, che perseguono ben altri scopi. Come nella vita quotidiana, i genitori devono stare attenti a queste persone che utilizzano chat, newsgroup, posta elettronica e ogni altro mezzo tecnologico per attirare l'attenzione dei minori con tutti i pericoli che ne possono derivare.

I RISCHI DELLA RETE

Per utilizzare tranquillamente gli strumenti e le opportunità della Rete, molte aziende, istituzioni e associazioni stanno promuovendo iniziative in questa direzione. *Pollicino nella Rete*, ideata da **Symantec**, vuole sensibilizzare genitori e bambini sulla cultura della sicurezza per una navigazione senza rischi. A tale scopo, è stata svolta un'indagine più approfondita, in collaborazione con l'associazione I.C.A.A. *International Crime Analysis Association* per capire quali sono i bambini più a rischio. Da questa inchiesta è emerso che quelli compresi tra 8 e 13 anni sono sensibilmente più a rischio e che i pedofili si avvicinano a loro usando *nickname* ispirati a fumetti famosi per attirare la loro attenzione. Cosa fare per difenderli? Installare un software che li protegga, configurare il motore di ricerca in modo adeguato e stare accanto ai propri figli quando navigano in Rete. **MICO**

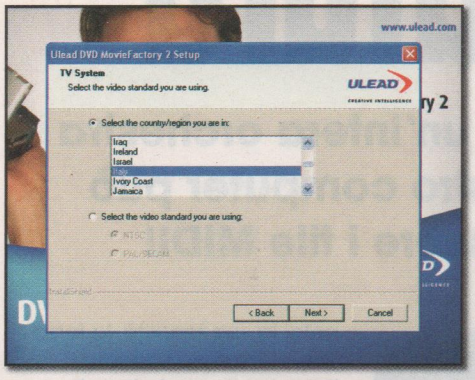
MOTORI DI RICERCA

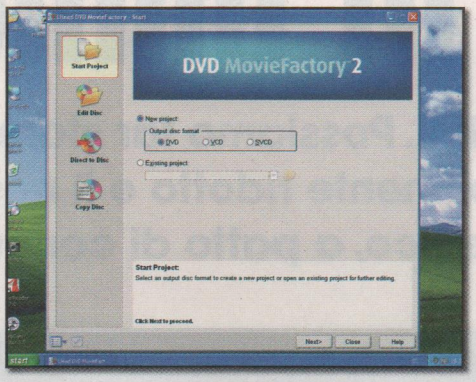
Vediamo come proteggere le nostre ricerche in Internet. **Google**: selezioniamo *Preferenze*, scegliamo *Usa livello massimo di filtraggio* e cliccare sul pulsante *Salva Preferenze*. **Yahoo**: clicchiamo su *Avanzata*, nella sezione *Filtro famiglia* clicchiamo sul link *Preferenze*. Facciamo clic sul link *Modifica*, scegliamo *Filtra i risultati della ricerca Web e dei file multimediali con contenuto per adulti*, premiamo *Salva* per proseguire nella ricerca. **Virgilio**: clicchiamo sul pulsante *Trova*, selezioniamo *Protezione familiare*, inseriamo la password da noi prescelta e tutte le altre informazioni che ci vengono richieste. Premiamo *Attiva* per concludere e salvare. **MSN.it**: premiamo *Cerca* e scegliamo *Impostazioni*, selezioniamo nella sezione *Ricerca sicura* l'opzione *Completo* per filtrare contenuti di testo e immagini a carattere sessuale esplicito. Premiamo infine il pulsante *Salva*.



IL NOSTRO PRIMO FILMATO CON DVD MOVIEFACTORY 2

PROGRAMMA COMPLETO





1 Installiamo **DVD MovieFactory 2** dal CD allegato alla rivista. Questo programma è completo e non presenta limiti d'uso. Chi vuole, può provare la versione 4, più avanzata, per 30 giorni prima di acquistarla. **Scegliamo le impostazioni per l'Italia.**

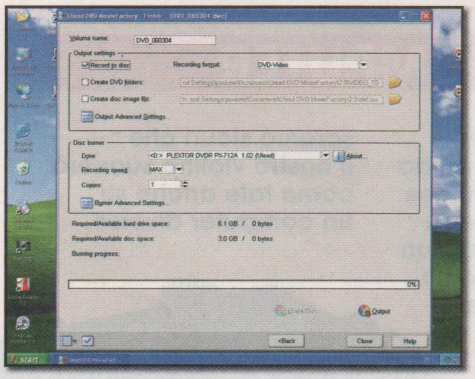
2 Per creare il nostro primo DVD possiamo usare file video già memorizzati nel disco fisso, preferibilmente in formato MPEG, *acquisire* il video direttamente da una scheda di acquisizione oppure copiare un DVD già esistente. **Attenzione ai diritti d'autore!**

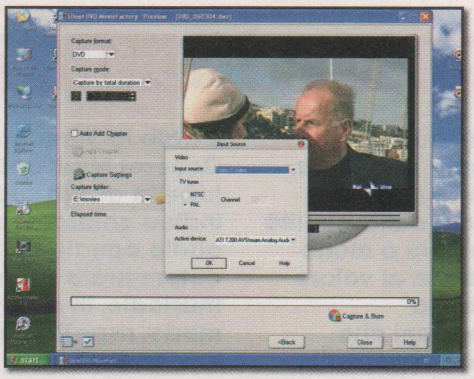
3 Se scegliamo di creare il nostro DVD partendo da file già memorizzati nel disco fisso, dobbiamo selezionarli uno a uno premendo **Add Video**. Ognuno di essi sarà visto come una voce principale del menu iniziale del DVD-video.

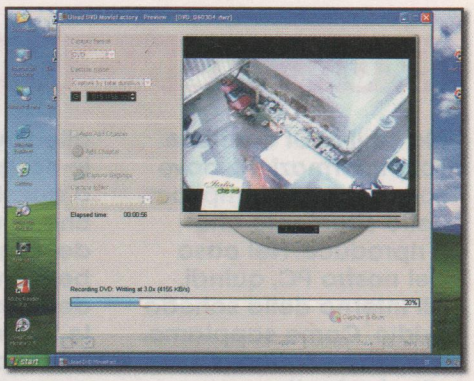
4 Può darsi che non ci interessi memorizzare tutte le sequenze che fanno parte di un file video. In questo caso, con l'opzione **Extract Video** possiamo inserire dei *marcatori* che indicano l'inizio e la fine delle sequenze che ci interessa includere nel DVD.

5 Un DVD, per essere comodo da vedere sui comuni lettori da salotto, deve essere *diviso in capitoli*. Una volta terminata l'operazione di assemblaggio, suddividiamo le scene come più ci aggrada, inserendo manualmente i capitoli dove preferiamo.

6 Non resta che dare un nome al nostro DVD, che farà bella mostra di sé quando lo inseriremo in un lettore. Possiamo usare uno dei *modelli* nella finestra a destra e modificare font e dimensioni del testo. Teniamo d'occhio anche la barra gialla in basso.







7 Non ci resta che memorizzare il frutto del nostro lavoro su un comodo DVD±R. **È preferibile usare supporti di tipo +R** se intendiamo usarli su un lettore DVD domestico. Se il nostro masterizzatore non ce la dovesse fare, possiamo usare comunque i -R.

8 Volendo, possiamo effettuare una registrazione *al volo*. In questo caso non dimentichiamoci di indicare al programma il tipo di sorgente video, il formato PAL e l'ingresso audio da usare (ATI T200), o non riusciremo a catturare proprio nulla!

9 Al termine della nostra registrazione la scrittura su DVD±R partirà in modo automatico. Per cui assicuriamoci di avere inserito un supporto vuoto nel masterizzatore. In caso di *DVD riscrivibili*, possiamo dire a MovieFactory di formattarli prima di scrivere.

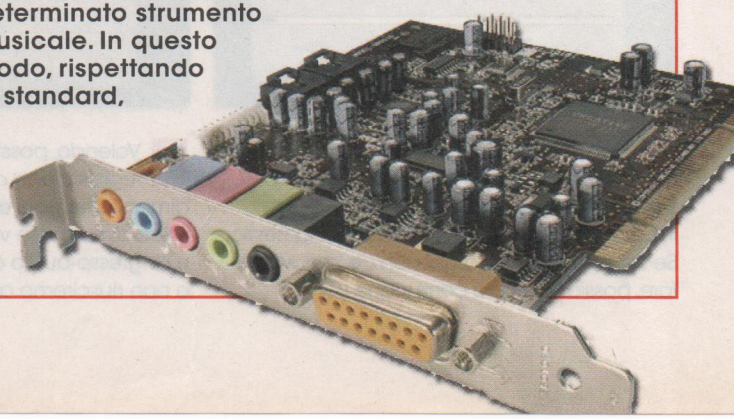
Musica in miniatura

Piccoli, anzi, piccolissimi. Possiamo far stare un'intera orchestra in uno spazio incredibilmente ridotto e il nostro computer può diventare un palcoscenico, a patto di conoscere i file MIDI!

Il protocollo MIDI nasce all'inizio degli anni '80 e da allora non ha subito praticamente variazioni. Già questo dovrebbe farci capire quanto sia stata brillante l'idea originale, ma che cos'è esattamente il MIDI? La sigla indica *Musical Instrument Digital Interface*, cioè *Interfaccia Digitale per Strumenti Musicali*. L'esigenza di una simile invenzione era data dalla necessità degli strumenti musicali elettronici di comunicare tra loro. In pratica, per creare sonorità più elaborate, si cercava di mescolare suoni provenienti da più strumenti controllandoli da una singola tastiera. Per ottenere questo risultato, il suono andava tradotto in un formato che potesse essere compreso dagli strumenti dell'epoca. Ecco perché i suoni MIDI, in realtà, non sono veri e propri *suoni*, ma piuttosto *informazioni*. Suonando una singola nota su una tastiera, infatti, il sistema raccoglie tutte le informazioni su quella nota: la sua tonalità, la forza con cui è stata suonata, il volume, la scala in cui si trova e così via. Tutte queste informazioni vengono trasferite, attraverso il protocollo MIDI, a un'altra tastiera che raccoglie le informazioni e riproduce la nota esattamente come è stata suonata. Grazie a questo sistema, non solo i tastieristi dell'epoca erano in grado di *pilotare* suoni provenienti da molti strumenti diversi, ma in seguito fu anche possibile creare interi brani da *ammassare* a decine nei floppy disk da 1,44 MB e portarli con sé per farli suonare ovunque. Il MIDI, quindi, ha dato vita a tantissime altre applicazioni musicali come, per esempio, il Piano Bar, il Karaoke e naturalmente i programmi per la creazione della musica attraverso il PC. Insomma: ancora oggi il MIDI è protagonista della musica. **MICO**

UN SUONO DIVERSO PER OGNI COMPUTER

Ma se il MIDI contiene solo informazioni, dove sono i suoni? Semplice: nello strumento che li riproduce. Nel caso del nostro PC, quindi, all'interno della scheda audio. Come sappiamo, esistono centinaia di schede diverse, ognuna con le proprie caratteristiche. Ecco perché le informazioni MIDI suoneranno in modo differente in base allo strumento che le esegue. Il problema, a questo punto, è che al di là della qualità del suono più o meno bello in base al valore della scheda, le informazioni che noi abbiamo pensato, per esempio, per un assolo di violino, potrebbero essere eseguite da un altro PC come una serie di colpi di tamburo! Ecco perché è nato lo Standard General MIDI: una rigida tabella di 128 suoni che indica chiaramente su quale canale si trova un determinato strumento musicale. In questo modo, rispettando lo standard, saremo sicuri che il nostro violino suonerà come tale anche su un computer diverso.



in edicola

ACQUISTARE, SCOPRIRE E USARE I NUOVI CELLULARI

Aprile - Anno 2006 - N. 3 € 4,90

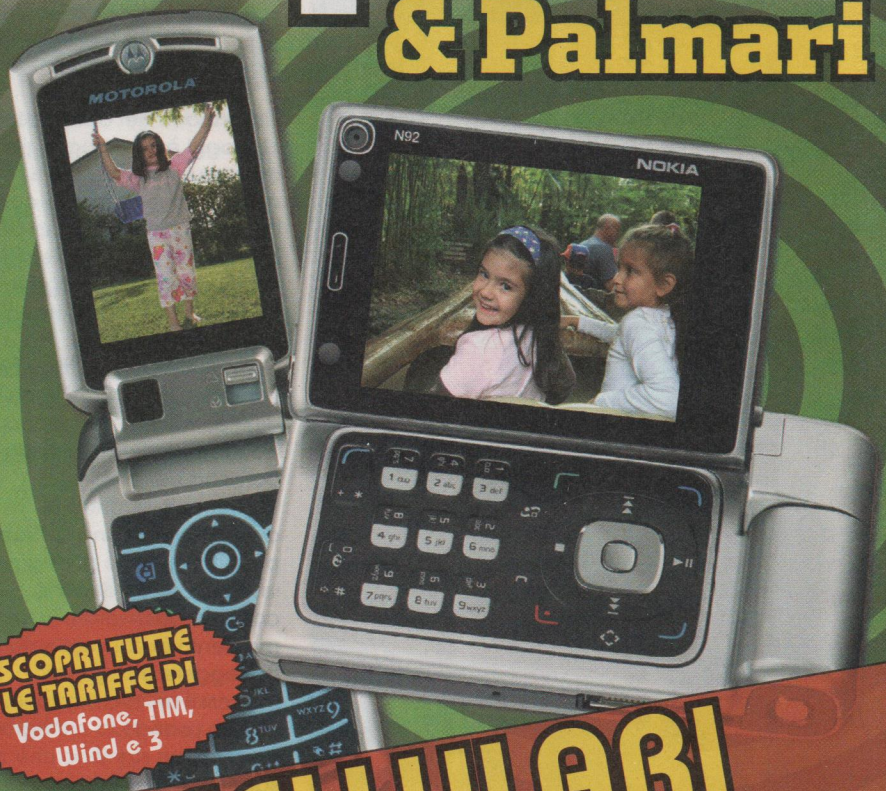
Smartphone & Palmari

GIOCHI FUTURI

Gli smartphone stanno diventando perfette macchine per giocare. E tra poco...

I MIGLIORI SOFTWARE

I segreti dei programmi indispensabili per i telefonini



SCOPRI TUTTE LE TARIFFE DI Vodafone, TIM, Wind e 3

FOTOCELLULARI

Le nuove frontiere della fotografia mobile

88 PRODOTTI PROVATI PER VOI!

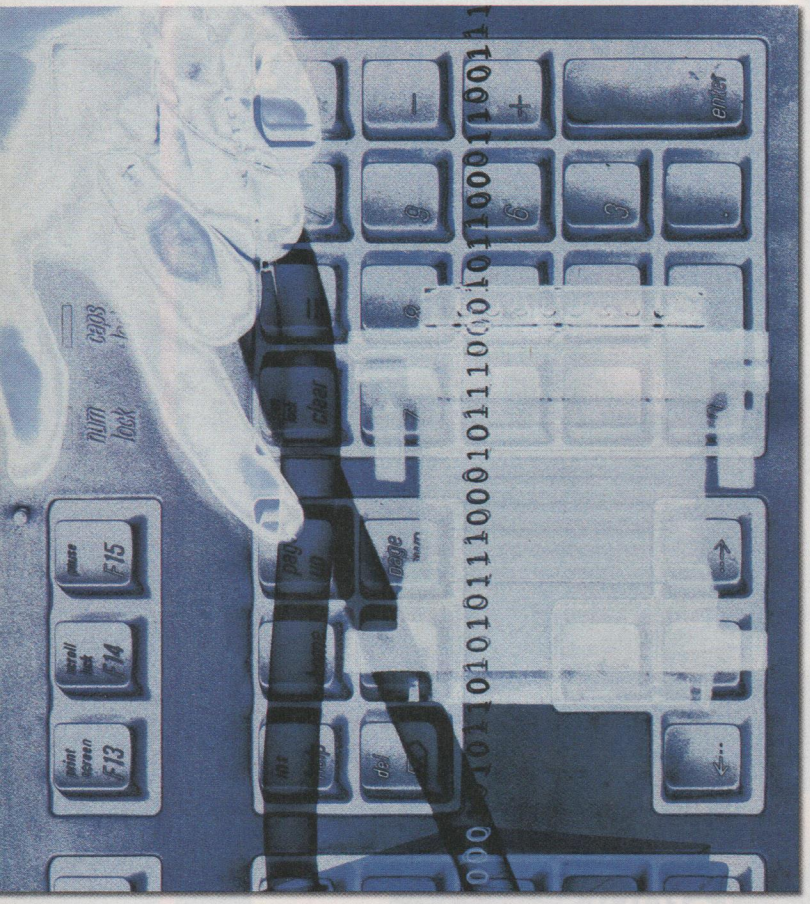
Smartphone & Palmari - Anno 2006 - nr. 3 - pubblicazione bimestrale registrata presso il Tribunale di Milano il 29/01/2002 al nr. 37 - Distribuzione: Parrini

60003
9 771826 570001

Future MEDIA WITH PASSION

Scritture segrete

Da secoli, militari e capi di Stato cercano di proteggere i loro messaggi usando la crittografia. Ora possiamo farlo anche noi grazie al nostro potente computer.



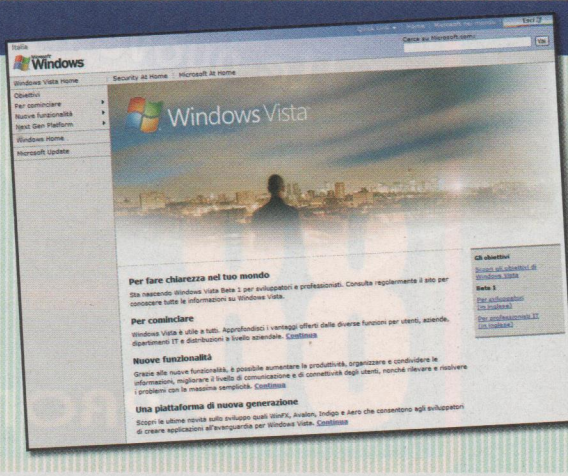
C'è una tecnologia che esiste da oltre 4.000 anni a cui dobbiamo l'invenzione dei computer e che oggi è usata ogni giorno da ognuno di noi senza nemmeno rendercene conto. Per indicarla, si usa una parola che deriva dal greco e significa *scrittura nascosta, segreta*: la *crittografia*. Diversamente da ciò che si pensa normalmente, la crittografia è molto diffusa: ogni volta che digitiamo il PIN del bancomat, quando facciamo un acquisto con carta di credito via Internet, quando ci colleghiamo a un sito Web protetto, quando proteggiamo un documento di Word con una password e in ogni momento in cui vogliamo proteggere da sguardi indiscreti un'informazione, stiamo usando la crittografia. Questo non significa che, senza saperlo, siamo tutti esperti di crittografia, ma solo che il suo utilizzo è molto più diffuso di quanto pensiamo. Per sfruttarla con lo scopo di proteggere la nostra privacy, però, occorre sforzarsi un po' e capire alcuni meccanismi che riguardano il suo funzionamento. Alla base di tutto ci sono tre cose: il testo da proteggere, detto *in chiaro*, il testo protetto, detto *in cifra* o *cifrato* e la *chiave di cifratura*: una parola chiave, una frase o una password che viene usata, insieme al testo in chiaro, per ottenere quello cifrato.

DUE ESEMPI STORICI

Le origini della crittografia si perdono nella notte dei tempi: ne parla persino la Bibbia, nel libro di Geremia. In questo testo viene spiegato un sistema di scrittura che prevede che le lettere del messaggio vengano scritte in ordine rovesciato: ogni lettera A del messaggio deve essere sostituita dalla Z, ogni lettera B deve essere sostituita con la Y e via dicendo. In questo modo, la frase *Ciao a tutti i nostri lettori*, diventa *XRZL Z GFGGR R MLHGIR OVGGLIR*. Questo sistema di proteggere le informazioni, che non fa uso

QUESTIONI VITALI

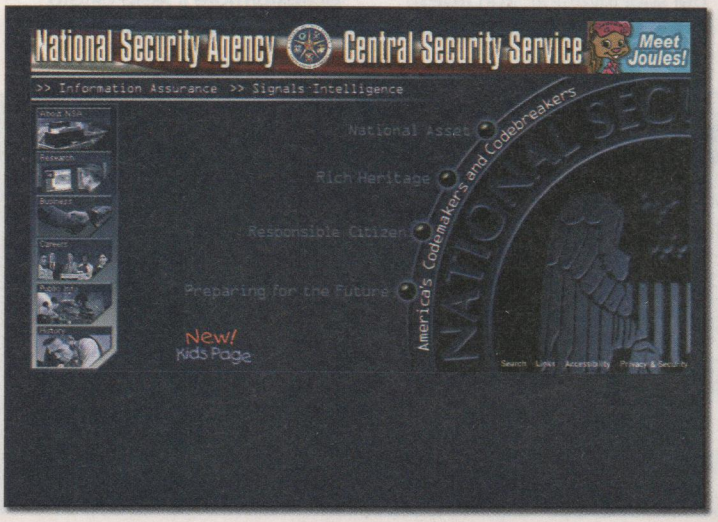
Proteggere i propri documenti con la crittografia sembra a molte persone un'inutile perdita di tempo. Gli allarmi sulla sicurezza e sulla privacy che vengono lanciati regolarmente sono spesso ignorati. Eppure, è ormai normale che i nuovi virus e programmi spia diffusi via Internet cerchino sempre di recuperare informazioni e documenti dai computer che infettano. Usando un sistema di crittografia si può avere la certezza che i documenti eventualmente sfuggiti al nostro controllo saranno illeggibili a qualsiasi malintenzionato. Allo stesso modo, la crittografia è utile per proteggere i nostri documenti quando il nostro PC viene usato da più persone, come negli uffici o in molte case. L'importanza della crittografia è tale che, con l'uscita del prossimo sistema operativo Windows Vista, queste funzioni di sicurezza saranno integrate all'interno del sistema stesso.



LA GUERRA DEI CODICI

Quando si parla di Seconda Guerra Mondiale, si pensa sempre a quella che, scoppiata nel 1939, si concluse nel 1945 con lo scoppio della seconda bomba atomica. In realtà, c'è un'altra guerra mondiale, segreta, scoppiata nel 1932 e terminata nel 1942, strettamente legata a quella più conosciuta: quella dei codici di cifratura. Tutto è nato quando, al termine della Prima Guerra Mondiale, la Germania mise all'opera i suoi tecnici per trovare un sistema di comunicazione sicuro tra i diversi comandi militari. Il prodotto di quello studio fu Enigma, una complicata macchina di cifratura che, almeno teoricamente, avrebbe dovuto essere inviolabile. Nel 1932, tuttavia, due matematici polacchi riuscirono a carpirne il segreto. La loro scoperta restò segreta a sua volta fino al 1939, quando, pochi giorni prima dell'attacco tedesco alla Polonia, venne messa a disposizione anche dei francesi e degli inglesi. In seguito, tali conoscenze vennero trasferite anche agli americani. Grazie al lavoro di matematici e tecnici che arrivarono a decifrare migliaia di messaggi al giorno, i generali alleati potevano essere informati dettagliatamente delle mosse tedesche e giapponesi. Al loro lavoro si devono diversi successi alleati, come la vittoria di Capo Matapan del marzo 1941, la sconfitta dei giapponesi nella battaglia di Midway, la realizzazione del piano dello sbarco in Normandia e molti altri episodi.

di una chiave, oggi ci fa sorridere: basta conoscere le operazioni svolte per ottenere facilmente qualsiasi testo in chiaro. Un altro esempio di codice simile è quello che venne chiamato *cifrario di Cesare*, usato in epoca romana: ogni lettera del messaggio in chiaro deve venire sostituita con una che la segue di un certo numero di posti, in base alla chiave. Per esempio, pensando di usare come chiave il numero 5, alla A corrisponde la F, alla B corrisponde la G e così via. Usando questo sistema, con la chiave 5, il nostro augurio ai lettori diventerà HNFT F YZYYN N STXYWN QJYYTWN. Ovviamente, anche questo sistema di cifratura, oggi, non ci permette alcuna sicurezza: ci sono solo 26 chiavi possibili, corrispondenti allo spostamento massimo delle lettere, in cui A=Z, B=A e via dicendo. Le chiavi possibili sono talmente poche da aver potuto dare problemi a qualche generale barbaro che non sapeva nemmeno leggere il latino, ma non sono certo un ostacolo al giorno d'oggi: si può anche procedere per tentativi, persino manualmente. Da allora, tuttavia, la crittografia ha fatto molti progressi e, nell'ultimo secolo, ha fatto addirittura passi da gigante.



Il sito dell'Agenzia per la Sicurezza Nazionale degli USA, www.nsa.gov, è ricco di indicazioni e immagini che riguardano la storia della crittografia.

DA ENIGMA AL DES

Nel ventesimo secolo, la crittografia, sulla spinta delle richieste di segretezza da parte di militari e capi di Stato, ha iniziato ad avere un'importanza sempre più elevata e sono state inventate diverse macchine che permettevano di cifrare e decifrare testi segreti in breve tempo e con sistemi sempre nuovi. Tra i molti successi della crittografia, il più famoso è senz'altro quello della macchina tedesca chiamata *Enigma*. Grazie all'uso di sistemi particolari, con chiavi di cifratura che cambiavano ogni 24 ore, le Forze Armate tedesche la ritenevano talmente affidabile da usarla in continuazione, per ogni loro comunicazione. Proprio questa sicurezza e l'importanza di »

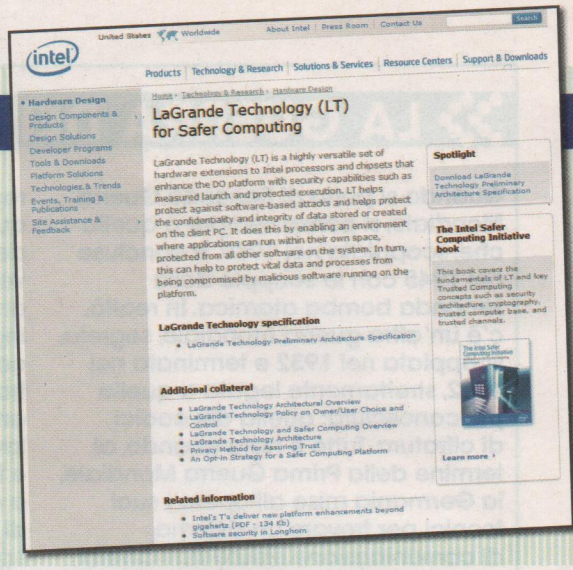
DAL TESTO AL CODICE

Proviamo a cifrare una frase usando il codice chiamato Campanile Germanico. Creiamo una scacchiera di 5 caselle per 5. Inseriamo nelle prime caselle la parola chiave, abolendo le lettere ripetute e, in quelle seguenti, le lettere mancanti alla parola chiave, in ordine alfabetico. Ora facciamo corrispondere ogni incrocio di colonna e riga alla lettera in chiaro.

	1	2	3	4	5
1	E	N	I	G	M
2	A	B	C	D	F
3	H	K	L	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

C	I	A	O	A	T	U	T	T	I
23	13	21	34	21	44	45	44	44	13

FRITZ L'ANTIPATICO



La nuova generazione di PC avrà al suo interno un piccolo circuito chiamato Fritz chip. Il suo scopo sarà quello di poter cifrare e decifrare velocemente le informazioni: unito a un sistema operativo capace di sfruttarlo, come Windows Vista, permetterà di cifrare l'intero contenuto del disco fisso senza rallentare l'esecuzione dei programmi. Questo circuito, tuttavia, risulta sgradito a molti: tra le sue caratteristiche c'è quella di contenere un numero identificativo univoco e di poter essere usato per cifrare anche i singoli file. Queste due caratteristiche permetteranno di identificare in modo sicuro il computer in cui verrà riprodotto un brano musicale, che si collegherà a un certo sito Web o che eseguirà un determinato programma: una gravissima violazione della privacy di ogni utente. Per ora, non sono servite a nulla le proteste dei movimenti per la libertà di espressione.

DAL CODICE AL TESTO

Osserviamo il messaggio cifrato nell'articolo con il codice di Cesare: HNFT F YZYYN N STXYWN QJYYTWN. Se ignoriamo il codice usato, possiamo comunque risalire al messaggio. Iniziamo a supporre che, nella parola YZYYN, le Y corrispondano a una lettera doppia come la T o la Z e procediamo per supposizioni. Più è lungo il messaggio, più sarà facile indovinarlo.

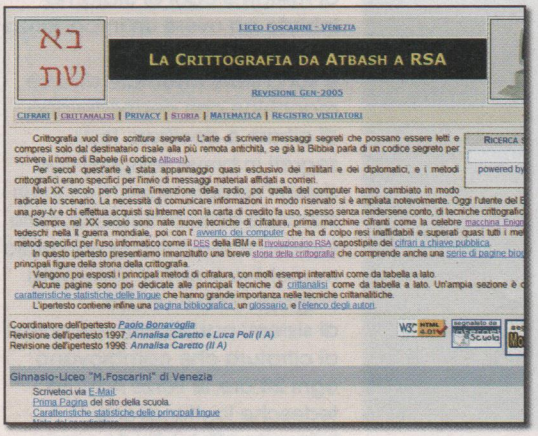
Mkby kwsmy, co rks nomspbkdy aeocdy
docdy, cos zbyzbsy lbkfy.
Mywzvswoxds!
Cmbsfsms exk wksv zob sxpybwkbms nov
dey oemmoccy.

mm=tt
Tkby kwsTy, co rks noTspbkdy aeocdy
docdy, cos zbyzbsy lbkfy.
Tywzvswoxds!
CTbsfsTs exk wksv zob sxpybwkbTs nov
dey oeTToccy.

scoprirne il funzionamento per risparmiare vite umane durante la guerra, diede l'impulso alle Forze Alleate per creare un gruppo di studio e decifratura dei messaggi tedeschi, chiamato *Ultra*. A Ultra partecipavano i matematici più brillanti a disposizione degli Alleati, tra i quali c'era Alan Turing, noto per aver posto le basi teoriche dell'informatica moderna. Il progetto degli Alleati, grazie a un po' di fortuna e a grandi intuizioni, riuscì a dare i frutti sperati: già nel 1942, i matematici che facevano parte del progetto riuscirono a decifrare oltre 80.000 messaggi tedeschi al giorno. Gli anni seguenti furono caratterizzati dalla ricerca di un sistema di cifratura che fosse inattaccabile alle analisi matematiche. Nel 1975, IBM presentò il sistema DES, ancora oggi il metodo di cifratura più usato in ambito informatico. Attualmente, malgrado il trascorrere del tempo, il DES e le sue modifiche successive sono ritenute sufficientemente affidabili da essere usate per le transazioni via Internet, la conservazione dei dati delle carte di credito e via dicendo. Lo svantaggio del DES, come di molti sistemi di crittografia, è che usa la stessa chiave sia per la codifica dei dati, sia per la decodifica.

RIVEST, SHAMIR E ADLEMAN

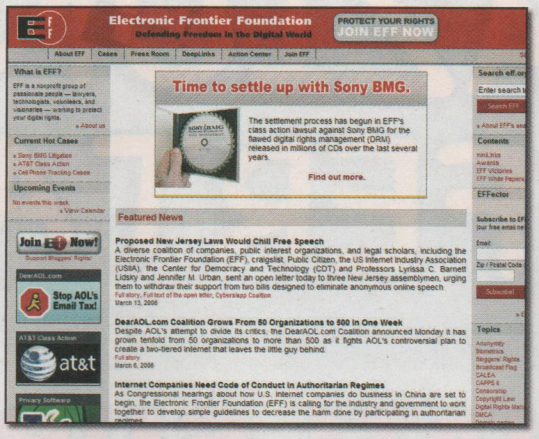
Una svolta alla crittografia si ebbe nel 1977, anno in cui nacque ufficialmente il sistema di crittografia RSA, dai cognomi dei suoi inventori: Ron Rivest, Adi Shamir e Leonard Adleman. Il suo principio di funzionamento non si basa più sulla codifica e decodifica del testo in chiaro per mezzo di una sola chiave, ma usandone due: una pubblica e l'altra privata. Grazie a complessi calcoli matematici, le due chiavi sono collegate tra loro, e un testo codificato usando una chiave non è reversibile tramite la stessa chiave: se si codifica un testo usando una chiave pubblica, è possibile tornare al testo originale solo usando la corrispondente chiave privata. In questo modo, possiamo generare le due chiavi e dare liberamente a tutti quella pubblica. Chi vuole inviarci un messaggio segreto usa quella pubblica per codificarlo e solo noi saremo in grado di trasformare il testo cifrato in quello originale. Allo stesso



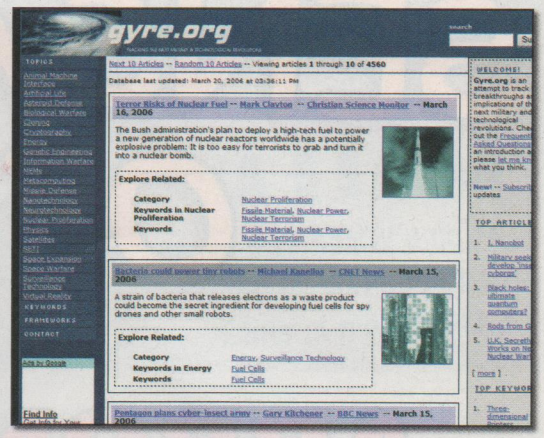
Se vogliamo studiare la crittografia, iniziamo visitando il sito del Liceo Foscarini di Venezia, www.liceofoscarini.it.

Per chi vuole approfondire l'argomento, un sito in italiano che offre spiegazioni sulla crittografia è www.tonycrypt.com.

modo, è possibile inserire in un testo una firma codificata con la nostra chiave privata e permettere ai destinatari di assicurarsi che sia stato proprio scritto da noi, controllando la firma tramite la nostra chiave pubblica. Ovviamente, il grande numero di calcoli necessari per codificare e decodificare i testi usando il sistema RSA, così come altri sistemi moderni di codifica, rende impossibile applicare manualmente questo genere di crittografia. Nel mondo dell'informatica, tuttavia, il sistema RSA e i suoi derivati hanno assunto sempre più importanza. Il livello di sicurezza che offrono è tale che, fino a qualche anno fa, il programma PGP, che usava il sistema RSA per codificare file e messaggi di posta, non poteva essere esportato dagli USA: era considerato un'arma di guerra.



Electronic Frontier Foundation, www.eff.org, si batte da anni per la diffusione della libertà di parola e della crittografia.



La crittografia fa parte da molto tempo dei temi trattati dal sito www.gyre.org, che si occupa di tecnologie militari.

QUESTIONI DI COSCIENZA

Nati per scopi militari, i sistemi di crittografia sono oggi al centro di diverse polemiche. Qualsiasi computer moderno può usare sistemi di crittografia per proteggere i documenti che ospita e chiunque, con un minimo di pratica, può svolgere queste operazioni in pochi minuti. Diversi tecnici ed enti di polizia a livello mondiale hanno più volte espresso preoccupazioni per la facilità con cui è possibile codificare messaggi, accusando i sistemi di crittografia, in particolare quello RSA, di favorire i terroristi, i pedofili e chiunque usi i computer in modo illegale. D'altra parte, occorre anche considerare che questi sistemi permettono di proteggere la propria privacy, un diritto di ogni persona, favorendo anche i gruppi di dissidenti nati in Paesi a regime totalitario. Così, malgrado qualche tentativo fatto in passato, oggi possiamo usare un sistema di crittografia senza alcun problema legale e nel Web sono disponibili moltissimi programmi adatti, spesso gratuiti. Possiamo codificare interi dischi fissi, alcuni singoli file, messaggi inviati per posta elettronica e così via. Anche usando il sistema di cifratura più complesso, quello RSA, la protezione dei nostri dati personali richiede solo pochi minuti e un minimo di attenzione. Ora non avremo più scuse: se qualcuno verrà a conoscenza dei nostri segreti, sarà solo colpa nostra. **MICO**

GLOSSARIO

CHIAVE ASIMMETRICA: sistema di cifratura che utilizza due chiavi distinte per cifrare e decifrare un testo.

CHIAVE PUBBLICA: una delle due chiavi dei sistemi a chiave asimmetrica da distribuire agli altri per comunicare con noi.

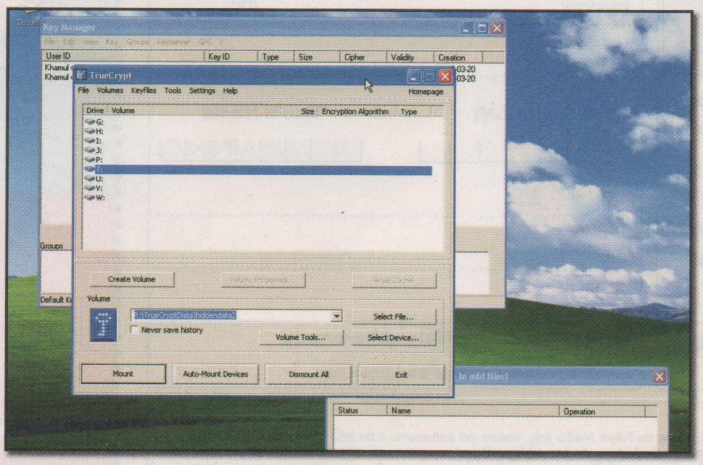
CHIAVE SIMMETRICA: sistema di cifratura che usa una singola chiave da mantenere segreta.

CRITTANALISI: disciplina che studia il sistema per decifrare un testo segreto senza conoscerne la chiave e il metodo usato.

TRASPOSIZIONE: insieme di operazioni prefissate che vengono svolte su un testo scambiando di posto alle lettere che lo compongono.

I PROGRAMMI NEL CD

Nel nostro CD trovate ben 3 programmi per la crittografia, tutti completi e gratuiti. Windows Privacy Tools è il corrispondente del famoso programma PGP, che usa un sistema di codifica con doppia chiave. Per una panoramica, vi rimandiamo al nostro articolo a pag.94. TrueCrypt è un programma di crittografia che ci permette di proteggere interi dischi fissi, usando i sistemi di crittografia a chiave singola più avanzati. Grazie a CryptoMX, un insieme di programmi basati su pagine Web, potremo studiare il funzionamento dei diversi sistemi di crittografia.



SENSAZIONALE OFFERTA!

ABBONATI SUBITO!

Rivista + Gioco completo + 13 CD per 13 numeri a soli € 50

CON UN RISPARMIO DEL 35%

OFFERTA SPECIALE ABBONAMENTO A IL MIO COMPUTER

Sì!
Desidero abbonarmi per un anno a
Il Mio Computer
Versione con CD + GIOCO COMPLETO
(€ 5,90 x 13 numeri) = **€ 50** (35% di sconto)

Modalità di Pagamento (Indicare con una crocetta)
❑ Versamento su bollettino postale che mi invierete
❑ Carta di Credito (dati riportati qui sotto)

Autorizzo l'addebito della Carta di Credito
❑ CartaSi ❑ Diners ❑ BankAmericard ❑ AmericanExpress
N° |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_| SCAD|_|_|/|_|_|
Firma del titolare.....

Se ti è più comodo, puoi inviare la cartolina via fax al numero 02/6428809

(Cognome) .....
(Nome) .....
(Indirizzo) ..... (Nr)
(Località) .....
(Prov.) (CAP) *(Data di Nascita)
|_|_| |_|_|_|_|_| GGMMAANNO
*(Tel.) .....
*(E-Mail) .....

Per informazioni - Ufficio abbonamenti
telefono: 02/6428135
e-mail: ilmiocomputer@imd-emd-group.com

INFORMATIVA AI SENSI DELL'ART. 13 DEL D.LGS. N. 196/2003
La informiamo che i dati raccolti saranno trattati, manualmente ed elettronicamente da Future Media Italy, titolare del trattamento e da IMD Srl, Responsabile del trattamento e resi disponibili agli incaricati preposti alle operazioni di trattamento finalizzate alla sua richiesta di iscrizione ai nostri servizi altresì trattati per eventuali proposte di rinnovo abbonamento, a fini statistici ed infine per aggiornarla su iniziative ed offerte commerciali anche per mezzo di posta elettronica. Le ricordiamo che ai sensi dell'art. 7 del D.Lgs. sopraccitato, ha il diritto di conoscere, aggiornare e cancellare i suoi dati, scrivendo in qualsiasi momento a Future Media Italia SpA c/o IMD Srl – Responsabile del trattamento Dati – via Guido da Velate, 11 – 20162 Milano. Nel caso non desiderasse ricevere comunicazioni commerciali da Future Media Italy o da suoi partner qualificati, lo segnali barrando la seguente casella ❑.
Consenso. Attraverso l'invio del modulo, Il/La sottoscritto/a, letta l'informativa sull'utilizzazione dei miei dati personali, ai sensi dell'art. 23 del D.Lgs. 196/2003, presta il suo consenso al trattamento dei dati personali per le finalità indicate nell'informativa.

35% DI SCONTO!

Ritaglia o fotocopia questo coupon, compilalo e invialo in busta chiusa a: **IMD srl Gestione Future Media Italy V. Guido da Velate, 11 - 20162 - Milano**